The context of Attacking the Network (AtN) / Network Disruption: An assessment of open source knowledge

Pierre Jolicoeur and Anthony Seaboyer

Prepared By:
Anthony Seaboyer
Royal Military College of Canada
Department of Political Science
National Defence
P.O. Box 17000, Station Forces
Kingston, Ontario, Canada K7K 7B4

RMC Project Manager:
Anthony Seaboyer
(613) 985-6111

Contractor's Document Number: CR-2014-XXXX
Contract Project Manager: Matthew A. Lauder, 613-541-5010 ext. 2558
SLA: 2009-0302-SLA
Annex No. 13009
PWGSC Contract Number:

Contract Scientific Authority: Matthew A. Lauder, DRDC – Toronto Research Centre
613-541-5010 ext. 2558

Defence Research and Development Canada
Contract Report
DRDC-RDDC-2015-C001
December 2014

Authors

Anthony Seaboyer and Pierre Jolicoeur
Royal Military College of Canada

Approved by

Matthew A. Lauder
Defence Scientist, DRDC Toronto

Approved for release by

Name of Document Review Chair
Chair, Document Review and Library Committee

Abstract

This report provides an overview of the state of knowledge in the open source (OS) domain in the field of Attack the Network (AtN) / Network Disruption (ND). By analyzing academic research results, as well as government documents and lessons learned from practitioners, this report identifies and assesses which knowledge currently exists on AtN / ND, how sufficient it is and where potential knowledge and information gaps and deficiencies occur. The report concludes with recommendations for further research into important AtN knowledge gaps that will enable the defence and security community to better function in the current and future operating environments.

Executive Summary

The increased emergence of failed and failing states has caused the defence and security community to face a steady increase in the number of networks engaged in violence. These networks are engaged in radicalization, fundraising for armed non-state actors (ANSAs), recruitment, attacks and even attempts to create state-like structures, as seen in the case of the Islamic State in Iraq and Syria (ISIS).

In times of scarce resources and rising threats, it is essential to determine how best to neutralize ANSAs domestically, as well as internationally.

This report provides an overview of the current state of knowledge in the Attack the Network (AtN) / Network Disruption (ND) open source (OS) domain. For this purpose, research reports, academic publications and military 'lessons learned' reports have been analyzed to identify existing knowledge and highlight current knowledge gaps. On the basis of the identified knowledge gaps, this study recommends specific areas for further research that will enable the defence and security community to better function now, and in the future.

The results of this research report generally confirm the findings of the DRDC Scientific Letter (SL), "Attack the network: Knowledge and information gaps and deficiencies,"[1] by Matthew A. Lauder, specifically:

1. Several AtN knowledge and information gaps, limitations and deficiencies exist, in particular in areas related to social and organizational entities and the human terrain; and

2. These gaps, limitations and deficiencies represent vulnerabilities that have the potential to undermine the broader C-IED capacity within the Canadian forces.

[1] Lauder, Matthew A. (2013): Attack the network: Knowledge and information gaps and deficiencies. DRDC/RDDC 2013 L3.

Introduction

The increased emergence of failed and failing states has caused the defence and security community to face a steady increase in the number of networks engaged in violence. These networks are engaged in radicalization, fundraising for armed non-state actors, recruitment (ANSAs), attacks and even attempts to create state-like structures, as seen in the case of the Islamic State of Iraq and Syria (ISIS). In times of scarce and limited resources, as well as rising threats, it is essential to determine how best to neutralize ANSAs networks, within both domestic and expeditionary contexts.

This report provides an overview of the current state of knowledge in the Attack the Network (AtN) / Network Disruption (ND)[2] open source (OS) domain. For this purpose, research reports, academic publications and military 'lessons learned' reports have been analyzed to identify existing knowledge and highlight current knowledge gaps. On the basis of the identified knowledge gaps, this study recommends specific areas for further research that will enable the defence and security community to better function now and in the future.

What is Attack the Network (AtN)

AtN can be defined as part of the Counter - Improvised Explosive Device (C-IED) capability. Within C-IED, AtN focuses on the offensive activities necessary to prevent networks from planning and implementing attacks, such as the use of IEDs. Defeat the Device (DtD) and Prepare the Force (PtF) focus on how to deal with threats from deployed IEDs. AtN is an offensive activity because it focuses on preventing networks from posing threat in the "left-of-boom" phase; that is, before attacks are even planned. DtD efforts are generally located in the immediate "left-of-boom" and "at-boom" phase; that is, immediately prior to and at detonation.[3]

AtN includes, but is not limited to, interdiction of resource acquisition, command and control, and planning, as well as the fabrication and transport of the device used for the attack. AtN commonly consists of three sub activities: (1) gaining intelligence, (2) building relationships, and (3) neutralizing the enemy. AtN is situated generally within the fields of network theory, network-based operations, irregular warfare, organizational theory and information strategy.

However, the term AtN has different meanings for different contributors to the C-IED effort, as well as for the larger defence and security community. "Many government experts believe that current AtN activities are biased towards lethal action directed at perceived "key" nodes in the enemy network. These lethal actions are necessary, but insufficient, to co-opt the local populace's support and disrupt the adversary's network."[4]

---

[2] In this report, the terms Attack the Network (AtN) and Network Disruption (ND) are considered to be synonymous. For ease of readership, AtN will be used throughout the report.

[3] Kinner, Scott (2013): Demystifying Attack the Network – A broader context, Marine Corps Gazette, January 2013.

[4] Toffler Associates and 4INNO (2010): Attack the Network – an Innovation Project, 29 Sept 2010.

Moreover, the intelligence community appears to understand AtN as a social network analysis problem, whereas soldiers in the field see it as kinetic action against network nodes, and other agencies have construction of local infrastructure and institutions in mind.[5] AtN, however, is not synonymous with, or specific to, the counter insurgency (COIN) environment.[6] In addition, it applies much more broadly to any adaptive networked threat that may challenge defence and security forces. While it is clear that it is essential to understand a network to determine how to fight it,[7] there is an obvious lack of a consistent operational framework, which would provide defence and security forces with a guide to utilizing existing lethal and non-lethal tools required by AtN.[8] Finally, this lack of operational framework has impacted defence and security training, resources, and an understanding of the overall effect forces can produce while engaging threat networks.

Accordingly, there are different definitions of what AtN encompasses. In a rather narrow and focus definition, AtN has been described as activities that "occur prior to an IED event that prevent the acquisition, assembly, transport, or placement of an IED and those activities that deter individuals from participating in any of these activities."[9] This can be seen as an unnecessarily limited focus on the C-IED field, which excludes the very similar fields of counter-insurgency, as well as operations against ANSAs. In this report, AtN is defined as:

> "A line of operation consisting of lethal and nonlethal actions and operations against networks conducted continuously and simultaneously at multiple levels (tactical, operational, and strategic), that capitalize on, or create key vulnerabilities and disrupt activities to eliminate the enemy's ability to function in order to enable success of the operation or campaign."[10]

The introduction of the AtN lexicon by the Joint Improvised Explosive Device Defeat Organization (JIEDDO) has addressed the lack of operational consistency by providing clear definitions of many AtN related terms, as well as describing one option to organize the process.[11] The first part of this research report identifies existing OS knowledge on AtN by providing an overview of some significant lessons learned, as well as research results. The second part identifies knowledge gaps,[12] limitations, and deficiencies, while the third part identifies the most promising areas for further research to enhance CAF AtN capabilities.

---

[5] Toffler Associates and 4INNO (2010): Attack the Network – an Innovation Project, 29 Sept 2010.

[6] United States Army, Maneuver Center of Excellence (2011): Attack the Network – An Operational Approach, January 2011.

[7] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

[8] Toffler Associates and 4INNO (2010): Attack the Network – an Innovation Project, 29 Sept 2010.

[9] Toffler Associates and 4INNO (2010): Attack the Network – an Innovation Project, 29 Sept 2010.

[10] Joint Improvised Explosive Device Defeat Organization (2011): Attack the Network Lexicon, May 2011.

[11] Joint Improvised Explosive Device Defeat Organization (2011): Attack the Network Lexicon, May 2011.

[12] Knowledge gaps are understood in the this report as a space characterized by little or no research results published regarding a question that is of high relevance to AtN.

The AtN knowledge space

> "It is essential to understand the war of context. Successful strategy needs to go beyond the weapon and address the issues that caused the mobilization of the insurgency or a terrorist's organization. This is the war of context."[13]

> "Understanding the context of irregular warfare is essential to creating effective efforts against fighting networks."[14]

> "In optional and limited wars, Western nations must learn how to fight in built-up and populated areas in ways that do as much as possible to deprive the enemy of the ability to force modern military forces to fight at the enemy's level, as well as in asymmetric ways that deprive conventional forces of their technical advantages and give the enemy the initiative."[15]

During many operations, attacks from networks in the form of IEDs pose the largest threat to civilians, as well as defence and security forces. The majority of casualties during the Canadian mission in Afghanistan were a direct result of IEDs.[16] Not only must AtN capabilities be improved to save lives of civilians and defence and security personnel,[17] they must also be improved to deal with the IED threats to the homeland.[18] To prevent these attacks from being implemented, offensive measures are essential. Successful offensive C-IED operations will attack and disrupt IED networks.[19]

The AtN knowledge space can be divided into the following subfields:

1. AtN operating environment changes;
2. Challenges in fighting networks;
3. The nature of threat networks;
4. Attack threat indicators;
5. Lessons learned on how to attack networks; and,
6. Necessary capabilities.

---

[13] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

[14] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

[15] Cordesman, Anthony (2007): Lessons of the 2006 Israeli-Hezbollah War. Washington, DC, Center for Strategic and International Studies Press, 2007.

[16] Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-012). 14 Oct 2009.

[17] Bekatoros, Nikolaos (2008): Exploring the Structure and Task Dynamics of Terrorist Organizations Using Agent Based Modeling, Naval Postgraduate School, Montery, December 2008.

[18] Joint Improvised Explosive Device Defeat Organization (2012): Strategic Plan 2012-2016, 1 Jan 2012.

[19] Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-012). 14 Oct 2009.

AtN operating environment changes

The increasing networked character of ANSAs[20] brings multiple changes to effective responses to national security threats.[21] These changes significantly increase the complexity of the task – both for personnel on the ground as well as for the planning of operations. Compared to traditional forms of warfare, AtN operations require a greater knowledge of the local environment and the human terrain, including but not limited to cultural and community structures.

When attacking networks, significant changes to the operating environment include:

1. **Information**
   AtN operations are by nature asymmetric and fall clearly into the field of irregular warfare. "Irregular warfare is about information, and a conflict between networks is truly a contest between information strategies."[22] For mission success when combating ANSAs, it is essential that information operations are appropriate, and timely. This has important implications for resource distribution because information needs not only to be collected but also processed in near real-time for use by combat forces when attacking threat networks.

2. **Decentralization**
   "Power is migrating to small, mostly non-state adversaries who can organize into sprawling networks more readily than traditionally hierarchical non-state actors."[23] In order to be able to react to for example local changes of individual network nodes in a timely manner and to avoid awaiting orders from multiple levels of command, small-unit decentralized operability is necessary.[24] Only small, decentralized units will be able to take rapid, self-organized action in response to movements of individual, loosely linked threat network nodes. Decentralization can also promote connectivity among units, enabling them to exchange locally relevant knowledge to respond to quickly evolving threat networks.

3. **Flexibility**
   Responding to ever-evolving threat networks, and the use of loose but centrally coordinated action, requires a high level of force flexibility. To be effective in engaging ever-changing networks, small units that are similarly flexible and can

---

[20] Martin, Brad et. al (2013): Assessment of Joint Improvised Explosive Device Defeat Organization (JIEDDO) Training Activity, RAND National Defense Research Institute, Santa Monica 2013.

[21] Minor, Mike M (2014): Counter-IED: A pervasive, global threat still remains, Vanguard, 2 December 2014. http://vanguardcanada.com/counter-ied-a-pervasive-global-threat-still-remains/

[22] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

[23] Manning, John D. (2010): Dark Networks, U.S. Army War College Strategic Research Project, February 2010.

[24] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

use comparable aspects of concealment and rapid strikes are required.[25] Flexibility in engagement strategies is also needed. Depending on the network, lethal and / or non-lethal measures will be required. Indirect elements of counter-insurgency (COIN) operations may be needed in combination with direct disruption operations.

Generally, it takes a network to fight a network. It is essential to create organizational structures that generate, process, and utilize vast amounts of information in near real-time while enabling decentralized command and flexible operations in the theatre.

Current challenges to AtN

The OS AtN knowledge space describes a wide variety of challenges facing the current AtN effort. While changes have been introduced, more must be done to conduct effective AtN operations. Deficiencies must be corrected within the areas of available resources, training, intelligence gathering, knowledge, relationships and Techniques, Tactics and Procedures (TTPs):

1. **Resources**
   Forces engaged in AtN operations lack the necessary resources to navigate the local cultural landscape, which is essential in order to gain valuable intelligence from the population, as well as their support.[26] A lack of equipment, facilities and skill-sets can prevent forces from overcoming a threat network's influence over the local population.[27] For example, AtN operations require sufficient access to interpreters who can adequately communicate with the local populace in a form that builds reliable and trust-worthy relationships. Additionally, dedicated vehicles for counter IED (C-IED) teams and necessary force protection must be readily available for rapid deployment.[28]

2. **Training**
   Much of current training is either ineffective or irrelevant for AtN, and does not provide the skills needed to coopt or undermine an IED network[29] or diminish its influence over the local population.[30] Soldiers report a lack of access to and time for training in AtN skills. Existing instruction focuses on lethal operations and lacks training in non-lethal approaches[31] such as information operations.[32]

---

[25] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

[26] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

[27] Toffler Associates and 4INNO (2010): Attack the Network – an Innovation Project, State of the Art Report, April 2010.

[28] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

[29] Knoke, David (2013): "It Takes a Network": The Rise and Fall of Social Network Analysis in U.S. Army Counterinsurgency Doctrine, Connections, Volume 33, Issue 1, July 2013.

[30] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

[31] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

Insufficient local language skills are also an obstacle to building rapport and trusted relationships.[33]

3. **Knowledge**
   Several knowledge generation and sharing / transfer issues are at play. First, AtN specific handbooks / guidebooks are not known to all personnel deploying. In addition, a poor transfer of knowledge across deployment cycles prevents building upon existing relationships, lessons learned and intelligence.[34] This results in limited knowledge about vehicle survivability in the local environment and protective levels of other equipment,[35] vulnerable points during patrols, and other best practices.[36]

4. **Intelligence**
   Forces lack training and sufficient resources[37] to effectively access, retain, synthesize, analyse and transfer intelligence across regions and deployment cycles.[38] Intelligence gathering is also difficult because members of threat networks are not easily distinguishable from the local population, and many threat network operations are hard to differentiate from legitimate activities.[39]

5. **Relationships**
   Forces face several challenges in building positive and trusting relations with local populations. First, it takes a significant amount of time for forces to build effective trust and rapport with local populations. Second, since local populations understand that defence and security forces are deployed for specific periods of time, there is a perception they will be left to defend themselves against threat networks.[40] Additionally, defence and security forces lack proper organization and training to build relationships that allow them to successfully isolate and target threat network actors from the local population.[41]

6. **TTP's**
   To increase AtN efficiency and flexibility in the theatre, TTP's on C-IED asset

---

[32] Newson, Robert A. (2014): America Has Forgotten How To Tell Its Side of the Story, Newsweek, 4 Dec 2014.

[33] Straziuso, Jason (2009): US Companies Send Translator To Afghanistan Who Are Old, Out Of Shape, Unprepared For Combat, Huffington Post, 22 August 2009**.**

[34] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

[35] Joint Task Force Afghanistan (2009): Theatre Lessons Report (07/09). Jul 2009.

[36] Army Lessons Learned Centre (2010): Lessons Synopsis Report (09-019). 19 Jan 2010.

[37] Flynn, Michael, et al (2010): Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan, Centre for a New American Security, January 2010.

[38] Land Force Doctrine and Training System (2010): Army Lessons Learned Centre Roll-Up Report January to June 2010, Kingston 2010, and Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

[39] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

[40] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

[41] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

> disposition during cordon and search (C&S) operations must be revised.[42] The lack of an AtN operational framework capturing the range of necessary AtN actions, as well as an integrated set of solutions satisfying AtN needs, leads to poor internal and community coordination.[43] For example, insufficient understanding of each community's complex cultural norms and needs may prevent exploitation of media opportunities or an understanding of which locals are most influential.[44] The lack of knowledge of AtN techniques often leads to an over reliance on lethal actions against threat networks.[45] This negative effect is further increased when leadership emphasizes and rewards conventional warfare skills and actions that are largely ill suited to AtN.[46]

Finally, AtN activities are complicated by threat network members' integration into the local community through cultural ties, existing relationships or employment. These connections not only enable them to influence locals, but also to threaten them with retaliation if they cooperate with AtN forces. Community integration also provides opportunities for threat network members to continually monitor AtN activities, learn TTP's and adapt their own operations, such as when placing an IED.[47]

The nature of networks

Several publications address, more generally, the phenomenon of threat networks. Understanding what threat networks are, and how they fight, is crucial to determining how to counter them.[48] This report defines threat networks as:

> "[N]etworks [that] are independent entities that use formal and informal ties to conduct licit or illicit activities and employ operational security measures and/or clandestine tradecraft techniques through varying degrees of overt, or more likely covert, activity to achieve their purposes"[49] and that threaten the security of a civilian population and / or defence and security forces.

Threat networks effectively execute planned operations not by orders but by providing guidance.[50] In contrast to AtN operations and traditional military structures, threat networks are highly flexible and agile as they can act almost independently from complex

---

[42] Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-010). 13 Aug 2009.
[43] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[44] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[45] Vogel, Steve (2009): Pentagon Lags in Developing Nonlethal Weapons, GAO Says, The Washington Post, 27 April 2009.
[46] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[47] Army Lessons Learned Centre (2010): Lessons Synopsis Report (09-019). 19 Jan 2010.
[48] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.
[49] Davis, Ian S./Worth, Carrie L./Zimmerman, Douglas W. (2010): A Theory of Dark Network Design. Naval Postgraduate School, Monterey.
[50] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

chains of command.[51] Threat networks are often aware of C-IED activities and exploit their knowledge by targeting responses to previous attacks.[52] Threat networks plan ambushes specifically targeting these C-IED teams[53] and often create conditions to force patrols to move tightly together, which increases the effect of an IED.[54] Threat networks' public statements are often inconsistent with their own practices. For example, they may publically denounce western values. However, they use state-of-the-art, western technology and social media platforms to achieve their goals.[55] To effectively engage threat networks, it is essential to study more closely how threat networks organize and function, as well as how they exploit socio-cultural and technological factors.

Threat networks are designed to buffer themselves from environmental hostility while fulfilling their goals and objectives.[56] "The level of hostility in the environment and the requirement for secure coordination of work determine the dark network's design state."[57] In order to determine the best form of engagement, it is helpful to focus on six design aspects of threat networks: that of (1) security, (2) agility, (3) resilience, (4) direction setting, (5) control, and (6) capacity.[58] If a threat network does not keep these aspects in balance, it risks network collapse and, ultimately, failure. Therefore, understanding how threat networks are designed can provide a conceptual construct for network interdiction.[59]

As the environment is always changing, threat networks must constantly adapt to the new situation. As a result, threat networks evolve over time.[60] If a threat network can be kept off balance and pushed towards a boundary, a vicious cycle leading to failure of the threat network can be triggered.[61] For example, a threat network may trade efficiency for secrecy, and this will significantly affect its output. AtN activities can target either the external dimension (e.g., by increasing the hostility of its environment) or the internal dimension (e.g., by influencing the secure coordination of cooperation) of a threat network.

---

51 Davis, Ian S./Worth, Carrie L./Zimmermann, Douglas W. (2011): A Theory of Dark Network Design (Part One), Small Wars Journal, 14 March 2011.

52 Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-012). 14 Oct 2009.

53 Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-017). 7 Nov 2007.

54 Army Lessons Learned Centre (2010): Lessons Synopsis Report (10-006). 23 Aug 2010.

55 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

56 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

57 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

58 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

59 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

60 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

61 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

To identify, appreciate and influence a threat network, it is essential to understand its operating environment.[62] "Understanding the environment that the network had configured itself to maximize operations within and then changing it to make the configuration a mismatch will affect the mode of operation and / or the methods of communication and potentially illuminate the network."[63] "Mitigating the antecedent conditions that enable dark networks to operate creates conditions that are unfavourable to achieve their desired purpose."[64]

Threat indicators

A significant portion of the AtN knowledge space addresses threat indicators – especially for IEDs. Many lessons learned reports are intended to enable knowledge sharing / transfer to prevent past methods of attack from being exploited again. A selection of major threat indicators includes:

1. **General IED threat indicators**
   Based on past attacks, it is known that IEDs are often planted near water sources or wells to ease device burial and concealment.[65] Chokepoints and terrain canals are also frequently used for attacks.[66] Threat networks attempt to mask the placement of IEDs or mines with goatherds[67] or children asking for water.[68] Cellphone calls made by individuals at the main entrance of camps have also preceded attacks.[69] Even cyclists should be carefully observed because they have been used to launch attacks.[70]

2. **Suicide Vehicle-Borne (SVB) IED threat indicators**
   Vehicle activity that has preceded attacks include pulling over and then aggressively approaching,[71] double U-turns,[72] or dangerous head on approaches with on-coming traffic.[73] SVBIED attackers are usually male, aged 20 to mid-30, and the sole occupants of a vehicle.[74] Tinted windows will often be used to hide

---

[62] Michael M. Phillips (2008): In Afghanistan, Getting to Know the Neighbors is Half the Battle, The Wall Street Journal, July 18, 2008.
[63] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.
[64] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.
[65] Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-013). 24 Sept 2007.
[66] Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-002). 9 May 2007.
[67] Army Lessons Learned Centre (2007): Lessons Synopsis Report (06-059). 16 Feb 2007.
[68] Army Lessons Learned Centre (2010): Lessons Synopsis Report (10-006). 23 Aug 2010.
[69] Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-053). 06 Nov 2006.
[70] Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-046). 28 Sept 2006.
[71] Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-008). 17 Aug 2007.
[72] Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-053). 06 Nov 2006.
[73] Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-005). 8 Jun 2007.
[74] Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-008). 17 Aug 2007.

how many occupants are in the car.[75]

3. **False safety indicators**
   SVBIED attacks often show no consideration for loss of civilian life or property damage.[76] Attacks are often conducted in congested areas, such as construction zones[77] or other urban areas with considerable pedestrian and vehicle traffic.[78] "The presence of civilians, sites of cultural significance, or the use of new vehicles cannot be used to gauge the likelihood of an attack."[79] Often a driver will show no signs of intent before launching the attack.[80]

How to attack networks

The most significant focus of the AtN knowledge space addresses how to effectively attack threat networks. Research and lessons learned concerning successful network attacks can be divided into the following areas: (1) understanding the operation, (2) organizing the attack, (3) engaging the threat networks, (4) assessing the operation, and (5) reducing effects of planned attacks.

Understanding the operation

1. **Mission**
   As a first step, it is essential that defence and security forces involved exactly understand the campaign and specific intent of the commander.[81] This includes understanding all areas of responsibility and interest.[82]

2. **Limitations**
   Secondly, it is important that forces understand the capabilities and limitations of their own team as well as those of their allies[83] and cooperation partners,[84] including indigenous forces.[85]

---

[75] Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-005). 8 Jun 2007.
[76] Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-057). 15 Feb 2007.
[77] Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-005). 8 Jun 2007.
[78] Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-057). 15 Feb 2007.
[79] Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-053). 06 Nov 2006.
[80] Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-050). 16 Oct 2006.
[81] Joint Improvised Explosive Device Defeat Organization (2011): Attack the Network Lexicon, May 2011.
[82] Joint Improvised Explosive Device Defeat Organization (2011): Attack the Network Lexicon, May 2011.
[83] North Atlantic Treaty Organization (2011): Commanders' and Staff Handbook for Countering Improvised Explosive Devices, August 2011.
[84] Fiore, Franco (2012): Counter-IED Technologies, Trends and Capabilities: Adopting a Multinational Cooperation Approach, Counter-IED report, Summer 2012.
[85] Centre for Army Lessons Learned (2009): Operation Enduring Freedom, IED-D Bulletin ll, No 09-45, August 2009.

3. **Operational environment**
   "The most significant part of the OE is almost always the people within it who belong to various networks."[86] Understanding the OE includes the complex local culture[87] with its unique mix of social factors, including ethnic groups, tribes, clans and family dynamics.[88] Only this level of insight will enable forces to learn about local populations planning attacks and how to influence them.[89] This knowledge must then lead to a campaign design, which "ensures the unit fully understands the OE and all the operational variables."[90]

4. **Threat network enabling context**
   To successfully attack a threat network, understanding the war of context is essential.[91] Attacking the factors leading to the emergence of the threat network is the key factor for long-term effective network neutralization. To understand these factors the focus should be on the social and human dimension of the local conflict.[92] An effective AtN strategy "needs to go beyond the weapon and address the issues that caused the mobilisation of the insurgency or terrorist organization. This is the war of context."[93] While this is a much more effective approach, it requires the political will to address the long term basic needs of the local population, thereby moving the key operational effort away from traditional warfare.

5. **Networks**
   Understanding threat networks require a basic knowledge of network concepts, and the ability to analyze and categorize networks.[94] To defeat the threat network, it is essential to have an understanding of network theory, including background, structure, and how networks relates to broader society.[95]

---

86 Training Brain Operations Center and U.S. Army Maneuver Centre of Excellence Attack the Network Teams (2012): Networks in the Operational Environment. How can we exploit them? Air Land and Sea Bulletin, Issue No. 2012-3, September 2012.

87 NATO International Staff Emerging Security Challenges (2014): Report of ISAF Briefing Day on Countering Improvised Explosive Devices, 27 January 2014.

88 Centre for Army Lessons learned (2009): CIED Bulletin III, No. 10-14, Dec 2009.

89 Elliott, Dan (2010): US troops train for both combat and conversation, Associated Press, 29 March 2010.

90 National Training Centre Fort Irvine (2010): NTC Operations Group Attack the Network Handbook, Fort Irwin 2010.

91 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

92 Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

93 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

94 Joint Improvised Explosive Device Defeat Organization (2011): Attack the Network Lexicon, May 2011.

95 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

Prepare the organization

1. **Prioritizing AtN**
   To achieve more effective network attacks, senior leadership must make AtN skill-sets a priority by developing doctrine, an operationalized AtN framework, and a definition of training standards that measures AtN skills. AtN principles must be embedded into leadership messages and officers must explain the link between AtN mission success and the survivability of forces members in the theatre.[96] As well, superiors need to conduct "road shows" and "spot checks" to reinforce AtN skills. These leaders need to explain that AtN requires a different skill set from that of the traditional warrior. Not all defence and security personnel are equipped with cultural awareness or are able to transition from the role of a soldier in a traditional war to a behavioural change agent with legitimate authority to use force.

2. **Creating better networks**
   Ultimately, in a network-to-network operation, the better network will win. Therefore, the goal of an AtN operation is to create a counter network that is more effective than the threat network. This can be achieved through enhanced information by empowering the intelligence war fighting function, developing an offensive mindset in all forces, and exploiting information operations opportunities.[97] To compete with a threat network, defence and security forces must adopt their increased connectivity and lower-level autonomy.[98] Governments may never entirely eliminate hierarchies, but decentralizing authority will enhance agility in attacks on networks.[99] Flattening AtN organization to share information laterally and reducing the "drag" at each layer of command will further enhance local information dominance.[100] Ideally, this will enable commanders to more rapidly adapt as conditions evolve and create more AtN opportunities because they have a better overall understanding of the OE.[101] A challenge will be to adopt a new mindset that emphasizes further connections.[102] Effective screening protocols should be implemented to identify team members with an aptitude for relationship building with indigenous

---

[96] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[97] National Training Centre Fort Irvine (2010): NTC Operations Group Attack the Network Handbook, Fort Irwin 2010.
[98] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.
[99] Zanani, Michele/Edwards, Sean (2001): The Networking of terrorism in the Information Age. In Networks and Netwars: The Future of Terror, Crime and Militancy, edited by John Arquilla and David Ronfeldt. Rand Corporation, Santa Monica.
[100] National Training Centre Fort Irvine (2010): NTC Operations Group Attack the Network Handbook, Fort Irwin 2010.
[101] National Training Centre Fort Irvine (2010): NTC Operations Group Attack the Network Handbook, Fort Irwin 2010.
[102] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

populations.[103] A collaborative targeting process, which uses digital systems to share real-time information, will also increase success.[104] Access to local language translators and cultural interpreters is critical for AtN. Translators must be screened, trained and embedded to be not only interpreters but also partners in the AtN effort so that the war fighters' experience with the local populace is changed.[105] For this to be successful, improved tactical language and cultural skills are necessary to augment the work of interpreters.[106]

3. **Optimizing AtN training and knowledge transfer**
   Training for AtN can be optimized by employing individuals capable of building community ties and informal networks, and by rewarding those who are successful in operating in fluid networked environments.[107] Simulation training with civilians should be a regular part of training as well as exposure to the local culture and population.[108] Social network analysis and network mapping must be components of regular training.[109] Lessons learned should be made accessible 24/7 by employing various multimedia, knowledge sharing platforms.[110]

Gaining intelligence

With the increased role of information in AtN operations, the need for accurate and timely accessible intelligence is paramount. Militarizing commercial collection and analysis technologies can help AtN forces distinguish threat network actors from the local population.[111] Providing patrols with passive facial recognition devices and tracking threat network employers with nano-sensors can provide AtN with multi-intelligence oversight if they have real-time access to an AtN knowledge base.[112]

[103] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[104] National Training Centre Fort Irvine (2010): NTC Operations Group Attack the Network Handbook, Fort Irwin 2010.
[105] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[106] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[107] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.
[108] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[109] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[110] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[111] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.
[112] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

Engaging networks

Support to friendly networks

Besides direct benefits of supporting local, likeminded and friendly networks[113] opportunities to gain valuable intelligence on threat networks[114] will emerge from building these relationships.[115] A lack of meaningful cooperation can have severe negative effects.[116]

Influence neutral networks

Those neutral to AtN goals should be encouraged to form future partnerships oriented towards common goals.[117] Thereby, "commanders must carefully asses the risk associated with the rapid exploitation of contacts / engagements in order to collect valuable information concerning IED networks" – especially as threat networks are capable of quickly extracting personnel and information from the theatre.[118] Creating rapport with the local population is crucial. "If they know you and trust you, they will tell you where to find / locate IED."[119]

Neutralize threat networks

Threat networks can be neutralized in the following ways:

1. **Attack the context**
   To effectively attack a threat network, the context that led local community members to join the threat network must be changed. "A strategy of context must involve the interagency powers in order to defeat the wider context in which these networks emerged."[120] Any attempt to attack a network will not bring long-term success if the local environment is not changed. "As in any other terrorist organization or oppressed society, a new leader or uprising can form because there has not been a change in the local environment.[121] "It is clear that irregular warfare cannot be separated from its inherent psychological,

---

113 Kilgore, Haimes et. al. (2012): Friendly, Neutral, And Threat Networks Show comparable Engagement Value, Air Land and Sea Bulletin, Issue No. 2012-3, September 2012.

114 Felisberto, Vitor (2014): What to expect from the Future of C-IED, Counter-IED report, Summer 2012.

115 Joint Improvised Explosive Device Defeat Organization (2013): Attack the Network, 3 March 2013.

116 Eisler, David F. (2012): Counter-IED Strategy in Modern War, Military Review, January-February 2012.

117 Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

118 Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-012). 14 Oct 2009.

119 Army Lessons Learned Centre (2010): Lessons Synopsis Report (10-003). 1 June 2010.

120 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

121 Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

cultural, and political aspects, and that any attempt to counter trheat networks must keep this at its core."[122] This has significant implications for the focus of missions, their duration, resources and type of forces involved. "The challenge then, for the political-military professionals, becomes what criteria are applicable, which aspects matter and how to maximize assets to fix or rebuild the State."[123]

2. **Change the environment**
On a more limited level changes to the local environment can impact the functioning of a threat network. "Understanding the environment that the network had configured itself to maximize operations within and then changing it to make the configuration a mismatch will affect the mode of operation and / or the methods of communication and potentially illuminate the network."[124] This includes affecting the funding and planning environment.[125]

3. **Attack the ideology**
The ideology threat networks use to justify violence is another effective target. "By educating terrorists on the fallacies within their beliefs and allowing them to express their religious beliefs" can affect cohesion and cooperation in a network."[126] Messages must be designed to resonate with the values, goals, and culture of the target audience.[127]

4. **Disrupt the narrative**
Effective disruption of a network's narrative and information campaigns are essential to AtN.[128] Counter threat network activities must "disrupt a network's external information flow while at the same time "claiming the space" with another message.[129]

5. **Persistent surveillance**
In neutralizing threat networks, surveillance can provide life-saving information. "Persistent surveillance by both manned an unmanned reconnaissance platforms

---

[122] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.
[123] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.
[124] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.
[125] Kinner, Scott (2012): Expanding Attack the Network, Air Land and Sea Bulletin, Issue No. 2012-3, September 2012.
[126] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.
[127] Joint Improvised Explosive Device Defeat Organization (2011): Attack the Network Field Guide, April 2011.
[128] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.
[129] Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

is extremely effective in striking an IED employer when synchronized with ground forces."[130]

6. **Exploit network misalignment**
The balance of a threat network can be disrupted by exploiting internal and external network misalignments. "Mitigating the antecedent conditions that enable threat networks to operate creates conditions that are unfavourable to achieve their desired purpose."[131] Efforts to create confusion, friction, gridlock, internal competition, and low performance can result in misalignment of a threat network's strategy, structure, processes, capabilities, reward systems and practices – leading to a decrease in secure communication and coordination capacity and ultimately impacting the efficiency of the threat network.[132]

7. **Exploit the "Oil Spot" methodology**
This method focuses on the links between the threat network's critical capabilities, requirements, and vulnerabilities by identifying the most vulnerable and critical nodes within a threat network.[133] This strategy first targets Tier II level intermediaries,[134] as they make Tier I targets more visible. In addition, Tier III targets will be forced to consolidate and reorganize.[135]

8. **Exploit warrant-based targeting**
Another method for AtN is warrant-based targeting that, together with prosecution task forces, can assist in attacking threat networks.[136]

9. **Develop threat-based counter-networks**
Finally, and not without significant negative implications, creating threat-based counter-networks can be an effective tool for attacking threat networks[137] as they are more difficult for the threat networks to observe and adapt to in complex environments.

---

[130] Centre for Army Lessons Learned (2009): Operation Enduring Freedom, IED-D Bulletin ll, No 09-45, August 2009.
[131] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.
[132] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.
[133] Asymmetric Warfare Group (2009): Attack the Network Part 1: Oil Spot Methodology, Fort George G. Meade 2009.
[134] Tier II targets can consist of false document providers, bomb makers, trainers, recruiters, weapon smugglers, media experts and financiers. The link between the ideological base and the center of gravity of networks is provided by Tier II targets.
[135] Asymmetric Warfare Group (2009): Attack the Network Part 1: Oil Spot Methodology, Fort George G. Meade
[136] Centre for Army Lessons learned (2009): CIED Bulletin III, No. 10-14, Dec 2009.
[137] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

Reducing the effect of planned attacks

1. **Information collection**
   To reduce the effect of IED attacks, all available sensors should be leveraged to obtain information on IED networks[138] and enable analysis.[139] GPS "Zone Alert Systems" can be an effective measure to warn forces when they enter dangerous areas if databases are updated with information on past attacks,[140] craters, potholes and other significant indicators.[141] Information collection can only be fully effective if all relevant information is passed on along all chains.[142] For this purpose, a comprehensive list of IED indicators must be continuously updated.[143]

2. **Planning**
   In planning operations the use of historical data[144] of threat networks attacks has proven very effective.[145] When planning troop movements, multiple crossing points, additional routes and contingency plans[146]are necessary to provide multiple options.[147] Routines should be avoided to prevent threat networks from exploiting patterns.[148]

3. **Movement**
   Troops in movement should use new or alternate routes whenever possible,[149] establishing a level of unpredictability.[150] [151] Wide spacing of convoy vehicles has often saved lives,[152] as "stand-off distance remains the single greatest blast mitigating factor."[153] Track discipline is also essential for safe travel.[154]

---

[138] Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-012). 14 Oct 2009.

[139] Smith, Thomas B./Tranchemontagne, Marc (2014): Understanding the Enemy, Joint Force Quarterly, No 75, 4th Quarter 2014.

[140] McAfee, John (2013): Intelligence Preparation of the Battlefield at the Company Level and Below, CIED Bulletin 13-9, September 2013.

[141] Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-010). 7 Sep 2007.

[142] Canadian Contribution Training Mission Afghanistan (2012): Incident Lessons Report (12-213). 15 Aug 2012.

[143] Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-008). 15 May 2009.

[144] Centre for Army Lessons Learned (2007): Handbook Tactical Site Exploitation and Cache Search Operations, May 2007.

[145] Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-004). 25 Mar 2009.

[146] Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-008). 15 May 2009.

[147] Army Lessons Learned Centre (2007): Lessons Synopsis Report (06-062). 6 Feb 2007.

[148] Canadian Contribution Training Mission Afghanistan (2012): Incident Lessons Report (12-213). 15 Aug 2012.

[149] Army Lessons Learned Centre (2007): Lessons Synopsis Report (06-059). 16 Feb 2007.

[150] Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-008). 15 May 2009.

[151] Army Lessons Learned Centre (2010): Lessons Synopsis Report (10-003). 1 June 2010.

[152] Army Lessons Learned Centre (2010): Lessons Synopsis Report (10-006). 23 Aug 2010.

[153] Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-057). 15 Feb 2007.

[154] Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-009). 24 April 2007.

Necessary capabilities for effective AtN

1. Improved understanding of all the relevant variables in the operating environment.[155]

2. "Synergy of rapid acquisition and fielding, operations and intelligence fusion and analysis, training,[156] weapons technical intelligence, and a whole-of-government approach"[157] focused on AtN.

3. Increased capacity to conduct fusion of intelligence products.[158]

4. Increased capability and capacity to build relationships with the local population.[159]

Recommended research to increase crucial AtN capabilities

Further research is not only essential to improve the effectiveness of current AtN efforts. Threat networks increasingly adapt[160] their strategies and techniques to AtN TTPs and improve, alter, and make bigger and deadlier devices.[161] To address AtN knowledge gaps, research is required in the following areas:

1. In-depth comparison of different types of threat networks;[162]

2. Threat-based counter networks and their role in AtN;[163]

3. Threat network warfare;[164]

4. Threat network activities;[165]

---

[155] National Training Centre Fort Irvine (2010): NTC Operations Group Attack the Network Handbook, Fort Irwin 2010.

[156] Blackburn, Jim (2012): Counter-IED Training and the Search for New Detection Technologies, Counter-IED report, Summer 2012.

[157] Joint Improvised Explosive Device Defeat Organization (2012): Strategic Plan 2012-2016, 1 Jan 2012.

[158] Canadian Contribution Training Mission Afghanistan (2012): Incident Lessons Report (12-213). 15 Aug 2012.

[159] Toffler Associates (2010): Attack the Network – An Innovation Project, 29 Sept 2010.

[160] Land Force Doctrine and Training System (2009): Army Lessons Learned Centre July to December 2009 Roll-Up Report, Kingston 2009.

[161] Whiteman, Shannon J. (2009): Improving Situational Awareness in the Counter-IED Fight with the Utilization of Unmanned Sensor Systems, Naval Postgraduate School, Montery 2009.

[162] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

[163] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

[164] Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

5. Threat network financiers and finance activities;[166]
6. Emerging AtN operational environments;[167]
7. Deployment of analysis and fusion teams and technology;[168]
8. Understanding of social and cultural aspects of the operational environment;[169]
9. Forms of effective threat network context influencing and changing;
10. Forms of effective threat network environment change;
11. Threat network engagement methods; and,
12. Forms of political violence.[170]

Conclusion

This report shows that the AtN OS knowledge space is broad and contains many lessons learned that can improve counter threat network capabilities. Significant knowledge exists regarding current challenges in AtN activities, IED threat indicators and also some aspects of how to fight networks.

However, these recommendations are not always feasible in the theatre. For example, the implementation of many lessons learned prevents troops from moving as agilely as needed for optimum AtN operations. There also appears to be a large focus both on the "post-boom phase" as well as the exploitation of kinetic-based lethal AtN methods.

However, only few sources describe the early stages of the "left-of-boom" phase and explain how threat networks can actually be neutralized. As a result, more research is needed on how this can be achieved. For example, how threat network contexts and environments can be influenced with available resources and in realistic timelines. Further research on the war of context is of utmost importance.

---

[165] Joint Improvised Explosive Device Defeat Organization (2012): Future R&D Capability Gaps, 27 Jan 2012.
[166] Joint Improvised Explosive Device Defeat Organization (2012): Future R&D Capability Gaps, 27 Jan 2012.
[167] Joint Improvised Explosive Device Defeat Organization (2012): Future R&D Capability Gaps, 27 Jan 2012.
[168] NATO International Staff Emerging Security Challenges (2014): Report of ISAF Briefing Day on Countering Improvised Explosive Devices, 27 January 2014, and Joint Improvised Explosive Device Defeat Organization (2012): Future R&D Capability Gaps, 27 Jan 2012.
[169] Joint Improvised Explosive Device Defeat Organization (2012): Future R&D Capability Gaps, 27 Jan 2012.
[170] Sageman, Marc (2008): A Strategy for Fighting International Islamist Terrorists, Annals of the American Academy of Political and Social Science, Vol. 618, July 2008.

AtN knowledge – with the exception of a few studies and documents – appears to be rather scattered and unorganized leading to the proposition of "catch all" approaches towards AtN that make it ultimately ineffective and not feasible. There seems to be a lack of a holistic, comprehensive, and systematic approach to the challenge of attacking threat networks.

To enhance the survivability of defence and security forces from threat networks, it is noted that further research on the following broad categories / areas is required: (1) threat network types and alternate forms of networks, (2) threat network warfare, (3) threat network activities and financing, (4) social and cultural aspects of networks, and (5) how to influence threat network contexts and environments.

This research is in concurrence with the original report on Attack the network knowledge deficiencies and gaps, namely that: (1) several AtN knowledge and information gaps, limitations and deficiencies exist, in particular in areas related to social and organizational entities and the human terrain; and (2) these gaps, limitations and deficiencies represent vulnerabilities that have the potential to undermine the broader C-IED capacity within the Canadian Armed Forces.

References

Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-046). 28 Sept 2006.

Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-050). 16 Oct 2006.

Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-053). 06 Nov 2006.

Army Lessons Learned Centre (2006): Lessons Synopsis Report (06-057). 15 Feb 2007.

Army Lessons Learned Centre (2007): Lessons Synopsis Report (06-059). 16 Feb 2007.

Army Lessons Learned Centre (2007): Lessons Synopsis Report (06-062). 6 Feb 2007.

Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-002). 9 May 2007.

Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-005). 8 Jun 2007.

Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-008). 17 Aug 2007.

Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-009). 24 April 2007.

Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-010). 7 Sept 2007.

Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-013). 24 Sept 2007.

Army Lessons Learned Centre (2007): Lessons Synopsis Report (07-017). 7 Nov 2007.

Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-004). 25 Mar 2009.

Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-008). 15 May 2009.

Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-010). 13 Aug 2009.

Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-012). 14 Oct 2009.

Army Lessons Learned Centre (2009): Lessons Synopsis Report (09-010). 13 Aug 2009.

Army Lessons Learned Centre (2010): Lessons Synopsis Report (09-019). 19 Jan 2010.

Army Lessons Learned Centre (2010): Lessons Synopsis Report (10-003). 1 June 2010.

Army Lessons Learned Centre (2010): Lessons Synopsis Report (10-006). 23 Aug 2010.

Asymmetric Warfare Group (2009): Attack the Network Part 1: Oil Spot Methodology, Fort George G. Meade 2009.

Bekatoros, Nikolaos (2008): Exploring the Structure and Task Dynamics of Terrorist Organizations Using Agent Based Modeling, Naval Postgraduate School, Montery, December 2008.

Blackburn, Jim (2012): Counter-IED Training and the Search for New Detection Technologies, Counter-IED report, Summer 2012.

Canadian Contribution Training Mission Afghanistan (2012): Incident Lessons Report (12-213). 15 Aug 2012.

Cordesman, Anthony (2007): Lessons of the 2006 Israeli-Hezbollah War. Washington, DC, Center for Strategic and International Studies Press, 2007.

Centre for Army Lessons Learned (2007): Handbook Tactical Site Exploitation and Cache Search Operations, May 2007.

Centre for Army Lessons Learned (2009): Operation Enduring Freedom, IED-D Bulletin ll, No 09-45, August 2009.

Centre for Army Lessons learned (2009): CIED Bulletin III, No. 10-14, Dec 2009.

Davis, Ian S./Worth, Carrie L./Zimmerman, Douglas W. (2010): A Theory of Dark Network Design. Naval Postgraduate School, Monterey.

Davis, Ian S./Worth, Carrie L./Zimmermann, Douglas W. (2011): A Theory of Dark Network Design (Part One), Small Wars Journal, 14 March 2011.

Dean, Arleigh William (2011): Fighting Networks: The Defining Challenge of Irregular Warfare. Naval Postgraduate School, Monterey.

Eisler, David F. (2012): Counter-IED Strategy in Modern War, Military Review, January-February 2012.

Elliott, Dan (2010): US troops train for both combat and conversation, *Associated Press*, 29 March 2010.

Felisberto, Vitor (2014): What to expect from the Future of C-IED, Counter-IED report, Summer 2012.

Fiore, Franco (2012): Counter-IED Technologies, Trends and Capabilities: Adopting a Multinational Cooperation Approach, Counter-IED report, Summer 2012.

Flynn, Michael, et al (2010): Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan, Centre for a New American Security, January 2010.

Joint Improvised Explosive Device Defeat Organization (2011): Attack the Network Field Guide, April 2011.

Joint Improvised Explosive Device Defeat Organization (2011): Attack the Network Lexicon, May 2011.

Joint Improvised Explosive Device Defeat Organization (2012): Strategic Plan 2012-2016, 1 Jan 2012.

Joint Improvised Explosive Device Defeat Organization (2012): Future R&D Capability Gaps, 27 Jan 2012.

Joint Improvised Explosive Device Defeat Organization (2013): Attack the Network, 3 March 2013.

Joint Task Force Afghanistan (2009): Theatre Lessons Report (07/09). Jul 2009.

Land Force Doctrine and Training System (2009): Army Lessons Learned Centre July to December 2009 Roll-Up Report, Kingston 2009.

Kinner, Scott (2012): Expanding Attack the Network, Air Land and Sea Bulletin, Issue No. 2012-3, September 2012.

Kinner, Scott (2013): Demystifying Attack the Network – A broader context, Marine Corps Gazette, January 2013.

Kilgore, Haimes et. al. (2012): Friendly, Neutral, And Threat Networks Show comparable Engagement Value, Air Land and Sea Bulletin, Issue No. 2012-3, September 2012.

Knoke, David (2013): "It Takes a Network": The Rise and Fall of Social Network Analysis in U.S. Army Counterinsurgency Doctrine, Connections, Volume 33, Issue 1, July 2013.

Land Force Doctrine and Training System (2010): Army Lessons Learned Centre Roll-Up Report January to June 2010, Kingston 2010.

Lauder, Matthew A. (2013): Attack the network: Knowledge and information gaps and deficiencies. DRDC/RDDC 2013 L3.

Manning, John D. (2010): Dark Networks, U.S. Army War College Strategic Research Project, February 2010.

Martin, Brad et. al (2013): Assessment of Joint Improvised Explosive Device Defeat Organization (JIEDDO) Training Activity, RAND National Defense Research Institute, Santa Monica 2013.

Michael M. Phillips (2008): In Afghanistan, Getting to Know the Neighbors is Half the Battle, *The Wall Street Journal*, July 18, 2008.

Minor, Mike M (2014): Counter-IED: A pervasive, global threat still remains, Vanguard, 2 December 2014. http://vanguardcanada.com/counter-ied-a-pervasive-global-threat-still-remains/ Accessed 5 December 2014.

McAfee, John (2013): Intelligence Preparation of the Battlefield at the Company Level and Below, CIED Bulletin 13-9, September 2013.

Morganthaler, Jeffrey/Giles-Summers, Brandon (2011): Targeting: Social Network Analysis in Counter IED Operations. Monterey.

National Training Centre Fort Irvine (2010): NTC Operations Group Attack the Network Handbook, Fort Irwin 2010.

North Atlantic Treaty Organization (2011): Commanders' and Staff Handbook for Countering Improvised Explosive Devices, August 2011.

Newson, Robert A. (2014): America Has Forgotten How To Tell Its Side of the Story, *Newsweek*, 4 Dec 2014.

NATO International Staff Emerging Security Challenges (2014): Report of ISAF Briefing Day on Countering Improvised Explosive Devices, 27 January 2014.

Sageman, Marc (2008): A Strategy for Fighting International Islamist Terrorists, Annals of the American Academy of Political and Social Science, Vol. 618, July 2008.

Smith, Thomas B./Tranchemontagne, Marc (2014): Understanding the Enemy, Joint Force Quarterly, No 75, 4th Quarter 2014.

Straziuso, Jason (2009): US Companies Send Translator To Afghanistan Who Are Old, Out Of Shape, Unprepared For Combat, *Huffington Post*, 22 August 2009.

Toffler Associates and 4INNO (2010): Attack the Network – an Innovation Project, State of the Art Report, April 2010.

Toffler Associates and 4INNO (2010): Attack the Network – an Innovation Project, 29 Sept 2010.

Training Brain Operations Center and U.S. Army Maneuver Centre of Excellence Attack the Network Teams (2012): Networks in the Operational Environment. How can we exploit them? Air Land and Sea Bulletin, Issue No. 2012-3, September 2012.

United States Army, Maneuver Center of Excellence (2011): Attack the Network – An Operational Approach, January 2011.

Vogel, Steve (2009): Pentagon Lags in Developing Nonlethal Weapons, GAO Says, *The Washington Post*, 27 April 2009.

Whiteman, Shannon J. (2009): Improving Situational Awareness in the Counter-IED Fight with the Utilization of Unmanned Sensor Systems, Naval Postgraduate School, Montery 2009.

Zanani, Michele/Edwards, Sean (2001): The Networking of terrorism in the Information Age. In Networks and Netwars: The Future of Terror, Crime and Militancy, edited by John Arquilla and David Ronfeldt. Rand Corporation, Santa Monica 2001.